THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF 139 NORTH VIEW DRIVE BRANSON, MISSOURI 65616	**Case No. 20-SW-2073DPR (UNDER SEAL)**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeremy Bluto, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent with Immigration and Customs Enforcement (ICE)/Homeland Security Investigations (HSI), Kansas City, Missouri, Principle Field Office, and have been so employed since April 25, 2010. I am currently assigned as a criminal investigator for HSI. Prior to my current position, I was employed with U.S. Customs and Border Protection, Office of Border Patrol, as a Border Patrol Agent and a Supervisory Border Patrol agent for five years, and a Deputy Sheriff with the Taney County, Missouri, Sheriff's Department for three years. Prior to my employment in Missouri, I attended California State University, Fullerton, and received a bachelor's degree in Criminal Justice.

2. As part of this affiant's duties with ICE/HSI, I investigate criminal violations relating to child exploitation, child pornography, and coercion and enticement, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422.

3. The statements in this affidavit are based on my personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) are currently

located at 139 North View Drive, Branson, Taney County, Missouri 65616, a location within the Western District of Missouri.

4. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing possession, receipt, distribution, and/or production of child pornography, and coercion and enticement of a minor. The property to be searched is described in the following paragraphs and fully in Attachment A. This affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

5. This affiant has probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) involving the use of a computer, in or affecting interstate commerce, to receive, distribute, possess, and/or produce child pornography, and coercion and enticement of a minor are located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located in this property.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) relating to material involving the sexual exploitation of minors:

a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.

b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

d. 18 U.S.C. § 2422(b) prohibits a person from using the mail or any facility or means of interstate or foreign commerce, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense.

DEFINITIONS

7. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality;

(c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

3. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms "records," "documents," and "materials," as used herein, include all

information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transfer Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on this affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

10. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords individuals several different venues for meeting one another, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

13. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Google, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer and/or other electronic devices in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic

tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

CELLULAR PHONES AND CHILD PORNOGRAPHY

15. Based on this affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

16. Cellular phones ("cell phones") are exceptionally widespread. The Central Intelligence Agency estimates that in 2016 there were 416 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images, and the ability to access and browse the Internet.

17. In this affiant's training and experience, the ready availability and personal nature of cell

phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.

18. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES

19. Searches and seizures of evidence from computers and cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer-related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems and cell phones for criminal evidence is a highly

technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media).

21. Furthermore, because there is probable cause to believe that the computer, its storage devices and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, and 18 U.S.C. § 2422, they should all be seized as such.

BACKGROUND OF INVESTIGATION

22. On February 20, 2020, this affiant began an investigation based upon a lead received from the HSI Cyber Crimes Center (C3), Child Exploitation Investigations Unit (CEIU). This lead was created by CEIU based upon information from Kik. Kik reported that a user, username

"brianmagee8809," was involved in chat in which suspected images of child pornography or erotica were uploaded. Kik provided a portion of a chat log, between user "brianmagee8809" and an undisclosed user (hereinafter "User X"), and images uploaded during the chat on May 27, 2019. During the conversation, User X reported that she was a 12-year-old female. User X also uploaded two image files during the conversations. Kik sent the images, which they had already viewed, with the lead. This affiant reviewed the images, which both depicted a close-up of the exposed left breast of a female. No other parts of the body, including the face, were included in the image. Based upon what was visible in the two images, this affiant was unable to confirm the images to be of a minor less than 18 years of age. After User X uploaded these images, the "brianmagee8809" user stated, "I'm posting your pics." That concluded the portion of the chat log sent by Kik.

23. Kik Messenger, commonly called Kik, is a freeware instant messaging mobile app from the Canadian company Kik Interactive, available free of charge on iOS and Android operating systems. It uses a smartphone's data plan or Wi-Fi to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content after users register a username. Kik is known for its features preserving users' anonymity, such as allowing users to register without providing a telephone number; however, the Kik application logs user IP addresses, which the company can use to determine location.

24. On February 14, 2020, this affiant spoke with Florham Park Boro, New Jersey, Police Department (FPPD) Detective Sergeant Michael Neilan. Detective Neilan stated he was calling the Springfield, Missouri, HSI office that day because he was investigating a case where the suspect may reside in the Southwest Missouri area. Detective Neilan explained that a 14-year-old minor female (hereinafter "Jane Doe") who resided in New Jersey had engaged in a series of

conversations on Kik with an individual who went by username "brianmagee8809." Based upon their investigation, the IP address for "brianmagee8809" resolved back to 139 North View Drive, Branson, Missouri 65616.

25. FPPD forwarded a copy of their report to this affiant. According to the report, on May 26, 2019, FPPD patrol officers responded to a call for service due to Jane Doe overdosing on prescription medication. Jane Doe's parents reported that Jane Doe had not been acting like herself lately and was going through a break-up. Jane Doe was transported for medical care.

26. On May 28, 2019, FPPD Detective Geoffrey Rothrock and Detective Sergeant Brian Ford made contact with Jane Doe's mother. Jane Doe's mother reported that Jane Doe had not overdosed due to a break-up as she and Jane Doe's father originally believed. Jane Doe's mother reported that Jane Doe had been using Kik to have sexually explicit conversations, and to send sexually explicit images, to another Kik user with username "brianmagee8809." The "brianmagee8809" user threatened to send the sexually explicit images and videos of Jane Doe to her family and friends. Jane Doe's mother signed a consent to seize and search Jane Doe's cellular phone, an Apple iPhone.

27. The Morris County Prosecutors Office (MCPO) High-tech Crimes Unit completed a download of Jane Doe's cellular phone. Kik conversations between Jane Doe, username "imahaydayaddict mia," and "brianmagee8809" were located within the Kik application. The first conversation, or chat, was initiated on May 25, 2019. The "brianmagee8809" user compliments Jane Doe on her appearance and asks her age, which Jane Doe responds that she is 14 years old. The "brianmagee8009" user tells Jane Doe that he is 15 years old male. The "brianmage8809" user then asks Jane Doe where she lives, her dating history, if Jane Doe is a virgin, what sex acts Jane Doe has performed before, and for images of Jane Doe's "booty." Jane Doe tells him that

she does not send nude images to strangers, and "brianmagee8809" then sends an image of a nude male with his penis exposed. Jane Doe asks the "brianmagee8809" user if she can send one later and if he has "snap or smith." The "brianmagee8809" user responds that his Snapchat username is "Tyler_smith1785." The "brianmagee8809" user sends Jane Doe a video of herself, one that Jane Doe had sent to another Kik user, and threatens to post it if she does not send him images and videos. Jane Doe then sends images and videos of herself engaged in sexually explicit conduct. The "brainmagee8809" user becomes aggressive demanding more images and videos. Jane Doe continues to send images and videos that depict her nude breast, bottom, and vagina, as well as images and videos of Jane Doe engaged in sexual acts, for example, one depicted her inserting a hairbrush into her vagina. The "brianmagee8809" user makes statements such as, "I want to cum now," "Like sit up and spread them apart," "show me how you sucked his dick," "Now ride that brush," "if u just fuck it, I need to still see ur facial expressions and moaning," and "Find something a little bigger to use." Jane Doe repeatedly pleads with "brianmagee8809" to stop, telling him, "can you please j leave me alone now," "what happened to leaving me alone after I send an ass pic," "you're an awful person," "can you j stop," and "I like don't wanna do that." The "brianmagee8809" user continues and tells Jane Doe, "Alright well I guess I'll just post everything rn then." Jane Doe begs him to reconsider and he tells her they will talk later.

28. On the next day, May 26, 2019, the "brianmagee8809" user continues to coerce Jane Doe and demands more images and videos of her engaged in sexual acts with other people. Jane Doe finally tells "brianmagee8809" that she is considering killing herself because she feels trapped and she does not know what else she can do, to which he responds, "That's ur choice." Jane Doe tells "brianmagee8809" that she took half a bottle of her mother's pills.

29. Law enforcement also located another Kik conversation that occurred between Jane Doe

and an individual using username "t. Hollins Tyler Hollins," who identified himself as a 17-year-old male. The "t. Hollins Tyler Hollins" user initiated the conversation with Jane Doe on May 25, 2019, at the same time as the one with "brianmagee8809" was occurring. During the conversation with "t. Hollins Tyler Hollins," Jane Doe sends a video. Later in the conversation, Jane Doe tells "t. Hollins Tyler Hollins" that another Kik user (referring to "brianmagee8809") sent her the same video she sent "t. Hollins Tyler Hollins." Jane Doe further tells "t. Hollins Tyler Hollins" that the other user is blackmailing her, and "t. Hollins Tyler Hollins" tells Jane Doe to do whatever the user says as long as he deletes everything. Jane Doe increasingly becomes desperate and on May 26, 2019, tells "t. Hollins Tyler Hollins," "its either him exposing me or me killing myself and not having to deal with it I like don't have any other option." After that, "t. Hollins Tyler Hollins" encourages Jane Doe to continuing meeting the other Kik user's demands, and Jane Doe accuses him of being the same person.

30. The MCPO sent investigative subpoenas to Kik, Snapchat, and Google for subscriber information. On June 12, 2019, the MCPO received a return from Kik which disclosed the "brianmagee8809" user's IP address during the conversation with Jane Doe was 38.131.214.35 and the user's registered email address was "brianmagee999@gmail.com."

31. On July 18, 2019, the MCPO received a return from Snapchat, which reported the "Tyler_smith1785" account was created on May 23, 2019, from IP address 38.131.214.35, and the registered email address was "tsmith1425@gmail.com" with a display name of "Brian M."

32. Through the course of their investigation, MCPO identified that IP address 38.131.214.35 was registered to Leslie McCullough at 139 North View Drive, Branson, Missouri 65616.

33. The Kik lead received by this affiant also indicated that the "brianmagee8809" user's IP address on May 27, 2019, while chatting with User X was 38.131.214.35. On February 24, 2020,

this affiant sent an investigative subpoena for IP address 38.131.214.35 on May 27, 2019, between 00:18:55 hours and 00:23:25 hours, UTC, for subscriber information to Sho-Me Technologies, LLC based in Marshfield, Missouri. Sho-Me Technologies responded to the subpoena indicating the IP address was assigned to Taneynet Broadband, a wireless ISP in Branson, Missouri. This affiant forwarded the investigative subpoena to Taneynet Broadband for subscriber information. On February 26, 2020, a response was received from Taneynet Broadband. The subscriber was reported as Leslie R. McCullough with a service address of 139 North View Drive, Branson, Missouri 65616.

34. This affiant conducted a records search that showed that 139 North View Drive, Branson, Missouri 65616 was purchased by Brandon L. and Leslie R. McCullough on May 31, 2018. On April 15, 2020, this affiant conducted brief surveillance at 139 North View Drive. The affiant observed one vehicle at the residence on two occasions, approximately 2 hours apart. The vehicle was a 2009 Toyota Corolla, black in color, bearing Missouri license "CW5J9E." Missouri Department of Revenue records indicate the vehicle is registered to "McCullough, Brandon L and Leslie R." On April 23, 2020, this affiant conducted a second brief surveillance at 139 North View Drive and observed second vehicle, a white GMC Terrain bearing Missouri license "CS1S1P." Records indicate the vehicle is registered to "McCullough, Brandon Lane and Leslie Renee." Both vehicles are registered with the 139 North View Drive address.

PROBABLE CAUSE

35. Based on the above facts, this affiant believes probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or

which is or has been used as the means of committing a criminal offense, namely possible violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) including, but not limited to, the items listed in Attachment B.

Further Affiant Sayeth Naught.

JEREMY L BLU Digitally signed by JEREMY L BLUTO
Date: 2020.04.30 09:35:17 -05'

Jeremy Bluto
Special Agent
Homeland Security Investigations

Sworn to and subscribed to before me in my presence via telephone on this 30th day of April 2020.

THE HONORABLE DAVID P. RUSH
Chief United States Magistrate Judge
Western District of Missouri